

## **AMENDMENTS TO THE CLAIMS:**

The following listing of claims will replace all prior versions, and listings, of claims in the captioned Application:

### **Listing Of Claims:**

Claim 1 (currently amended):           A method for authenticating transferred data between a sender computer and a receiver computer over an open network, the method comprising the steps of:

establishing a first secure transmission of data between the sender computer and the receiver computer;

assigning a value to a variable N where the value of N is a positive number and defines a selected number of additional transmissions;

transmitting selected authentication information including [at least one] N number of token(s) and a checksum value from the sender computer to the receiver computer during the first secure transmission so as to allow the sender computer to authenticate itself, [the number of tokens being set to a variable N where N defines a selected number of additional transmissions and] each of the N number of token(s) [is] being a unique identifier;

transmitting an acknowledgment from the receiver computer to the sender computer, upon successful receipt and processing of the first transmission by the

receiver computer;

establishing at least one additional transmission of data between the sender computer and the receiver computer;

transmitting the data and the at least one token from the sender computer to the receiver computer during the at least one additional transmission;

comparing the [at least one] N token(s) transmitted from the sender computer during the additional transmission to each of the token(s) transmitted from the sender computer during the one or more previous transmission(s) to determine whether the most recent additional transmission is authentic; [and]

establishing a second secure transmission [during which] between the sender computer [transmits to] and the receiver computer [a second selected value of N, N number of tokens and a second checksum value to be used to authenticate the sender computer.];

assigning a second value to the variable N where the second value of N is a positive number and defines a second selected number of additional transmissions; and

transmitting the second value of N, a second value of N number of tokens, and a second checksum value to be used to authenticate the sender computer, from the sender computer to the receiver computer, each of the second N number of tokens being a unique identifier.

Claim 14 (currently amended): A method for securely transferring data between a client computer and a server over an open network, the method comprising the steps of:

establishing a first secure transmission between the client computer and the server which is encrypted;

assigning a preselected value to a variable N where the preselected value of N is a positive number and defines a selected number of additional transmissions;

transmitting selected authentication information including the preselected value of N number of token(s) and a checksum value from the client computer to the server during the first secure transmission so as to allow the sender computer to authenticate itself, [the number of tokens being set to a variable N where N defines a selected number of additional transmissions and] each of the N number of token(s) [is] being a unique identifier;

transmitting an acknowledgment from the server to the client computer, upon successful receipt and processing of the first transmission by the client computer;

establishing additional transmissions between the client computer and the server corresponding to the preselected number of tokens N;

transmitting the data, one of the preselected value of N number of token(s) and the checksum value from the client computer to the server during each additional transmission;

during each additional transmission, comparing the token transmitted from the client computer to the server during such additional transmission

to the corresponding token transmitted during the first secure transmission

to determine whether the additional transmission is authentic; [and]

establishing a second secure transmission [during which] between the client computer [transmits to] and the server [a second selected value of N, N number of tokens and a second checksum value to be used to authenticate the client computer.];

assigning a second value to the variable N where the second value of N is a positive number and defines a second selected number of additional transmissions; and transmitting the second value of N, a second value of N number of tokens, and a second checksum value to be used to authenticate the client computer, from the client computer to the server, each of the second N number of tokens being a unique identifier.

Claim 23 (currently amended):      A method for authenticating transferred data between a sender computer and a receiver computer over an open network, the method comprising the steps of:

establishing a first secure transmission of data between the sender computer and the receiver computer;

assigning a value to a variable N where the value of N is a positive number and defines a selected number of additional transmissions;

transmitting selected authentication information including [at least one] N number of token(s) and a checksum value from the sender computer to the receiver computer during the first secure transmission so as to allow the sender computer to

authenticate itself, [the number of tokens being set to a variable N where N defines a selected number of additional transmissions and] each of the N number of token(s) [is] being a unique identifier;

transmitting an acknowledgement from the receiver computer to the sender computer, upon successful receipt and processing of the first transmission by the receiver computer;

establishing at least one additional transmission of data between the sender computer and the receiver computer;

transmitting the data and the at least one token from the sender computer to the receiver computer during the at least one additional transmission;

comparing the [at least one] N token(s) transmitted from the sender computer during the additional transmission to each of the token(s) transmitted from the sender computer during the one or more previous transmission(s) to determine whether the most recent additional transmission is authentic; and

establishing a second secure transmission [during which] between the sender computer [transmits to] and the receiver computer [a second selected value of N, N number of tokens and a second checksum value to be used to authenticate the sender computer];

assigning a second value to the variable N where the second value of N is a positive number and defines a second selected number of additional transmissions;

transmitting the second value of N, a second value of N number of tokens,

and a second checksum value to be used to authenticate the sender computer, from the sender computer to the receiver computer, each of the second N number of tokens being a unique identifier; and

each of the additional transmissions being variable and adaptively selected, at least in part, based upon a set of criteria used in an algorithm to determine the number of additional transmissions, the criteria being selected from a group consisting of the frequency of transmissions between the sender computer and the receiver computer, the closeness of the sender computer to the source of the transactions, and the usage patterns of the sender computer.